

# ISE 2.0을 구성하고 AnyConnect 4.2 Posture BitLocker 암호화 암호화 암호화 암호화

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[ASA](#)

[Windows 7의 BitLocker](#)

[ISE](#)

[1단계. 네트워크 디바이스](#)

[2단계. 상태 조건 및 정책](#)

[3단계. 클라이언트 프로비저닝 리소스 및 정책](#)

[4단계. 권한 부여 규칙](#)

[다음을 확인합니다.](#)

[1단계. VPN 세션 설정](#)

[2단계. 클라이언트 프로비저닝](#)

[3단계. 상태 확인 및 CoA](#)

[버그](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 Microsoft BitLocker를 사용하여 엔드포인트의 디스크 파티션을 암호화하는 방법과 네트워크에 대한 전체 액세스를 제공하기 위해 Cisco ISE(Identity Services Engine)를 구성하는 방법에 대해 설명합니다. 단, 올바른 암호화가 구성된 경우에만 해당됩니다. AnyConnect Secure Mobility Client 4.2와 함께 Cisco ISE 버전 2.0은 디스크 암호화를 위한 상태를 지원합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA(Adaptive Security Appliance) CLI 컨피그레이션 및 SSL(Secure Socket Layer) VPN 컨피그레이션
- ASA의 원격 액세스 VPN 컨피그레이션
- ISE 및 포스처 서비스

## 사용되는 구성 요소

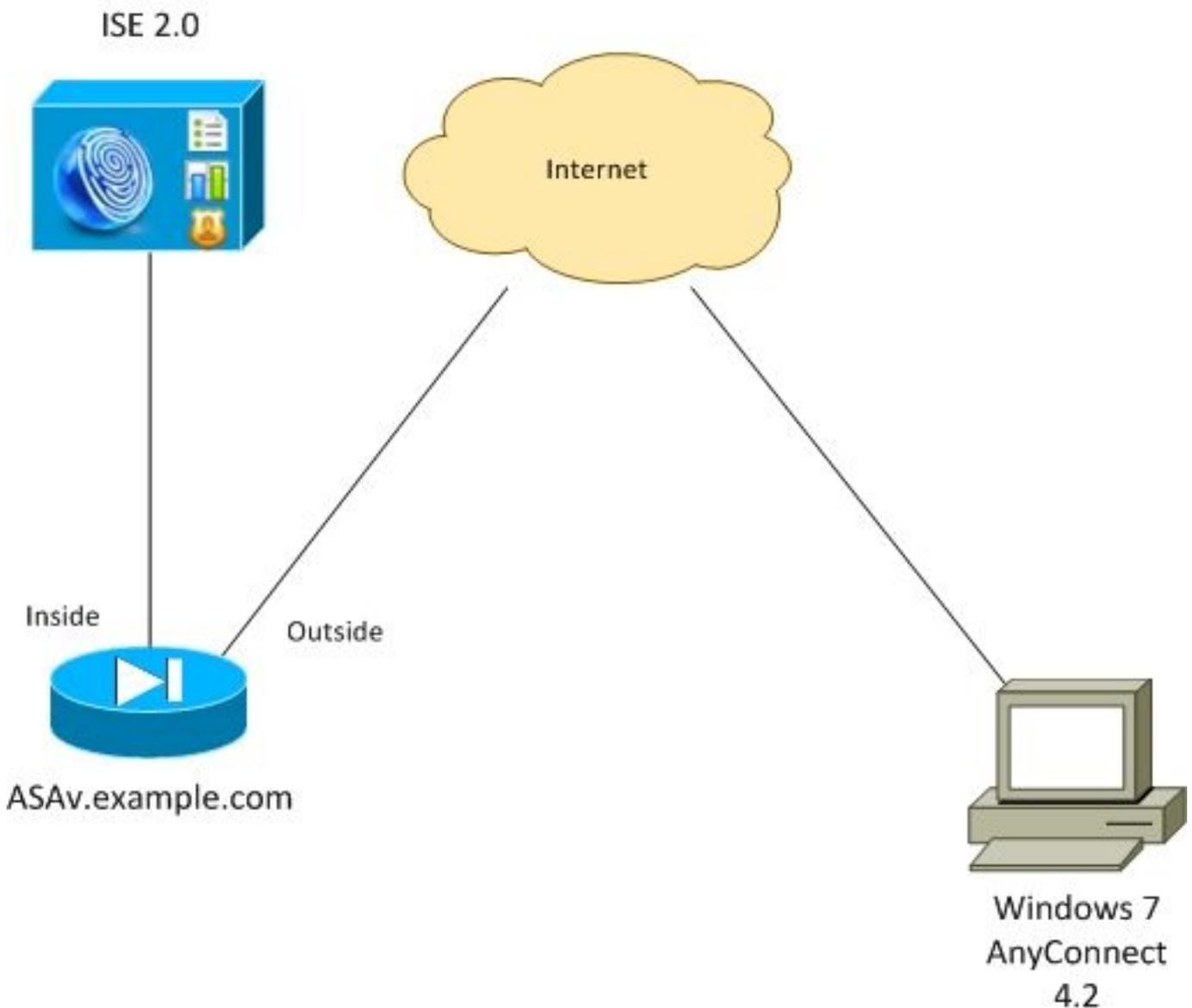
이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco ASA 소프트웨어 버전 9.2.1 이상
- Cisco AnyConnect Secure Mobility Client Version 4.2 이상이 포함된 Microsoft Windows 버전 7
- Cisco ISE, 릴리스 2.0 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 구성

### 네트워크 다이어그램



플로우는 다음과 같습니다.

- AnyConnect 클라이언트에서 시작된 VPN 세션은 ISE를 통해 인증됩니다. 엔드포인트의 상태

상태를 알 수 없습니다. 규칙 **ASA VPN 알 수 없음**이 적중되어 프로비저닝에 대한 세션이 ISE로 리디렉션됩니다.

- 사용자가 웹 브라우저를 열고 ASA에서 ISE로 HTTP 트래픽을 리디렉션합니다. ISE는 최신 버전의 AnyConnect와 함께 상태 및 규정 준수 모듈을 엔드포인트에 푸시합니다.
- 포스터 모듈이 실행되면 파티션 E:BitLocker로 완전히 암호화됩니다. 대답이 "예"인 경우 ISE로 보고서가 전송되며, ACL(전체 액세스) 없이 CoA(Radius Change of Authorization)를 트리거합니다.
- ASA의 VPN 세션이 업데이트되고 리디렉션 ACL이 제거되며 세션에 전체 액세스 권한이 있습니다.

VPN 세션이 예시로 표시됩니다. 다른 액세스 유형에 대해서도 상태 기능이 정상적으로 작동합니다.

## ASA

ISE를 AAA(Authentication, Authorization, and Accounting) 서버로 사용하여 원격 SSL VPN 액세스에서 구성됩니다. 리디렉션 ACL과 함께 RADIUS CoA를 구성해야 합니다.

```
aaa-server ISE20 protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE20 (inside) host 10.48.17.235
  key cisco

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
  address-pool POOL
authentication-server-group ISE20
accounting-server-group ISE20
  default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
  group-alias TAC enable

group-policy AllProtocols internal
group-policy AllProtocols attributes
  vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable

access-list REDIRECT extended deny udp any any eq domain
access-list REDIRECT extended deny ip any host 10.48.17.235
access-list REDIRECT extended deny icmp any any
access-list REDIRECT extended permit tcp any any eq www

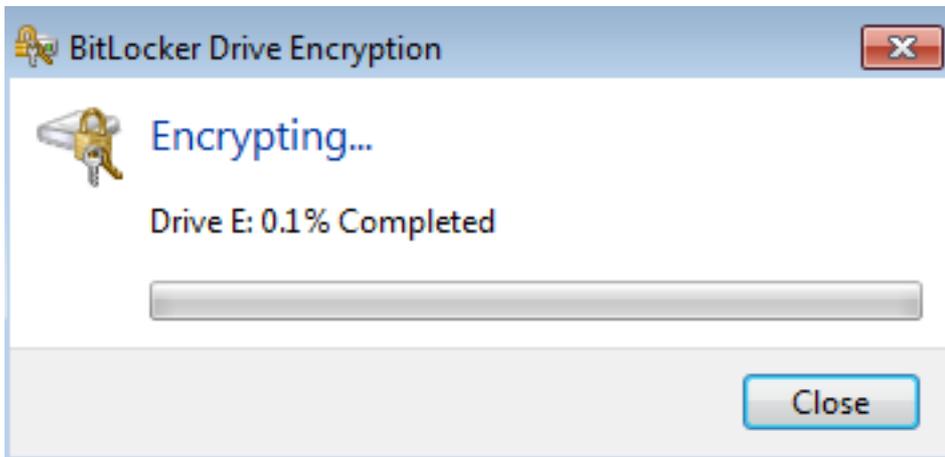
ip local pool POOL 172.16.31.10-172.16.31.20 mask 255.255.255.0
```

자세한 내용은 다음을 참조하십시오.

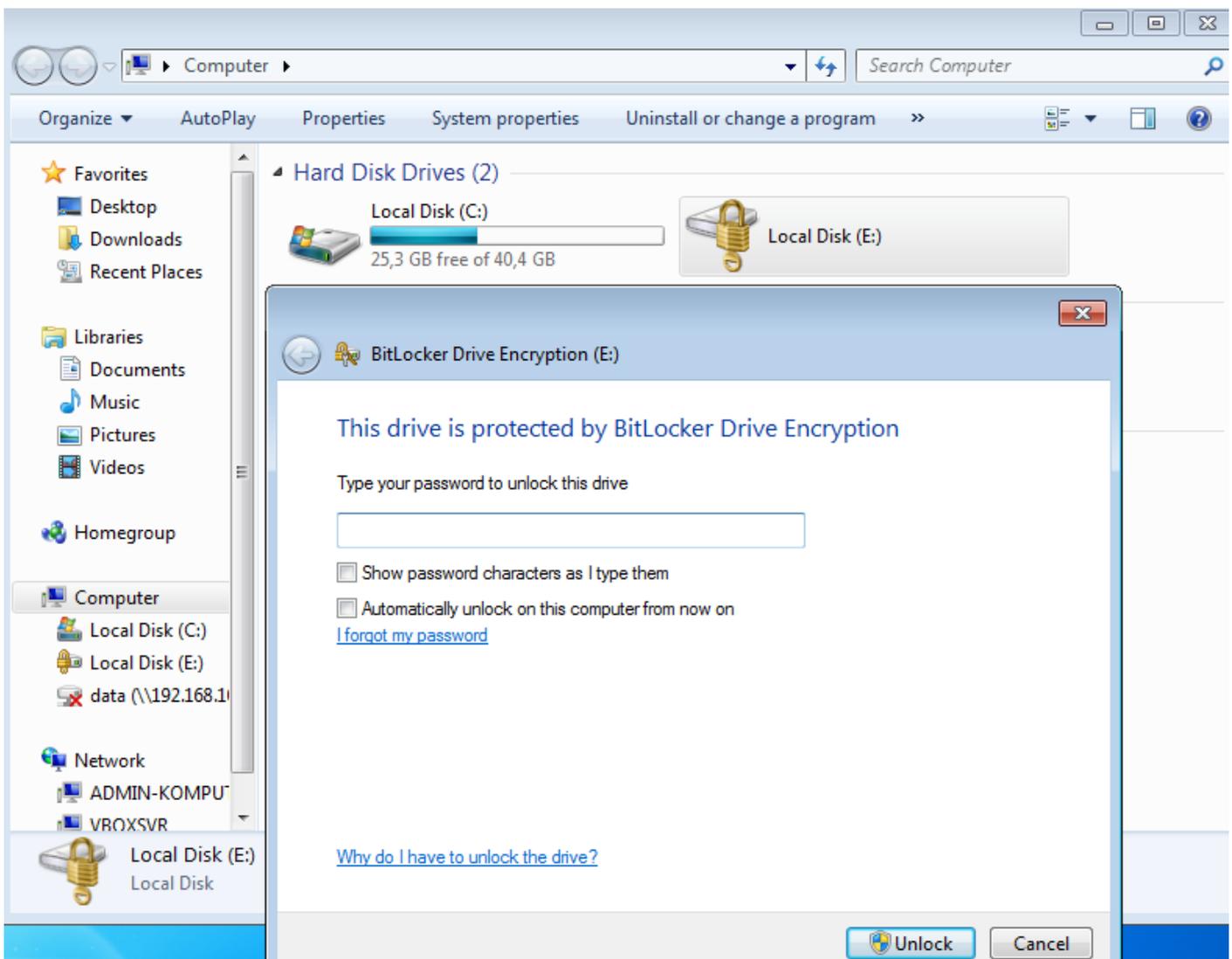
[AnyConnect 4.0과 ISE 버전 1.3 통합 컨피그레이션 예](#)

## Windows 7의 BitLocker

Control Panel(제어판) > System and Security(시스템 및 보안) > BitLocker Drive Encryption(BitLocker 드라이브 암호화)으로 이동하고 E를 활성화합니다. 파티션 암호화. 이미지에 표시된 대로 비밀번호(PIN)로 보호합니다.



암호화가 완료되면(비밀번호 프로비저닝을 통해) 마운트하고 이미지에 표시된 대로 액세스할 수 있는지 확인합니다.



자세한 내용은 Microsoft 설명서를 참조하십시오.

# ISE

## 1단계. 네트워크 디바이스

Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스), Add ASA with Device Type = ASA(디바이스 유형 = ASA가 있는 ASA 추가)로 이동합니다. 이는 권한 부여 규칙에서 조건으로 사용되지만 필수는 아닙니다(다른 유형의 조건을 사용할 수 있음).

필요한 경우 네트워크 장치 그룹이 존재하지 않습니다. 생성하려면 Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹)로 이동합니다.

## 2단계. 상태 조건 및 정책

상태 조건이 업데이트되었는지 확인: Administration(관리) > System(시스템) > Settings(설정) > Posture(포스처) > Updates(업데이트) > Update Now(지금 업데이트)로 이동합니다.

Policy(정책) > Policy Elements(정책 요소) > Conditions(조건) > Posture(포스처) > Disk Encryption Condition(디스크 암호화 조건)으로 이동하여 이미지에 표시된 새 조건을 추가합니다.

The screenshot shows the Cisco ISE configuration interface. The breadcrumb trail is: Policy > Policy Elements > Conditions > Results > Disk-Encryption Conditions List > bitlocker. The main configuration area is titled 'Disk Encryption Condition' and includes the following fields:

- Name: bitlocker
- Description: (empty)
- Operating System: Windows All
- Vendor Name: Microsoft Corp.

Below these fields is a table titled 'Products for Selected Vendor':

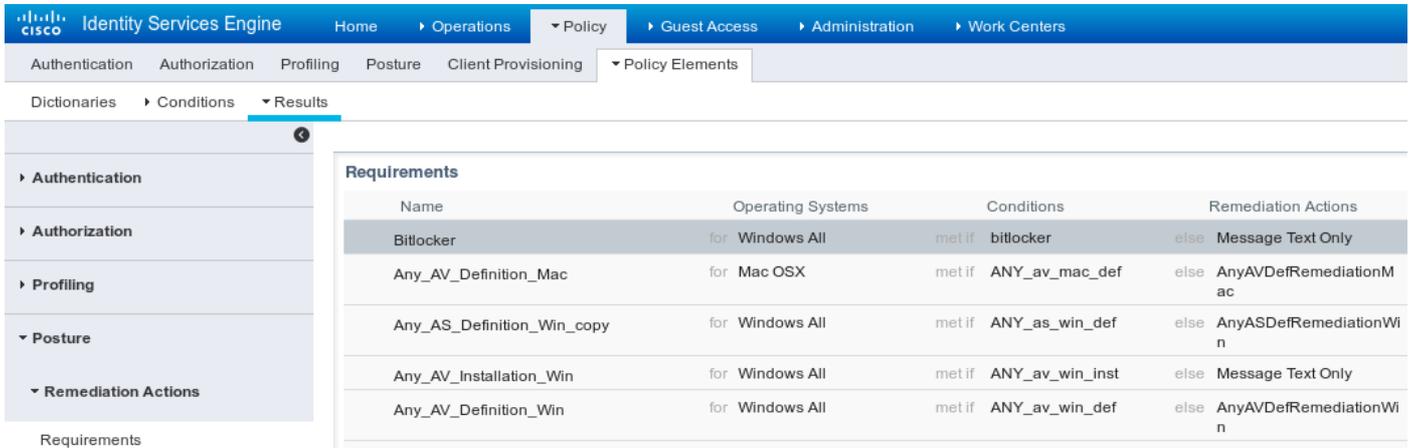
	Product Name	Version	Encryption State Check	Minimum Compliant Module Supp...
<input type="checkbox"/>	BitLocker Drive Encryption	10.x	YES	3.6.10146.2
<input checked="" type="checkbox"/>	BitLocker Drive Encryption	6.x	YES	3.6.10146.2

At the bottom, there is a checkbox for 'Encryption State' which is checked. Below that, there is a 'Location' dropdown menu set to 'Specific Locatio...', an 'E:' input field, and radio buttons for 'Fully Encrypted OR Pending Encryption OR Partially Encrypted'.

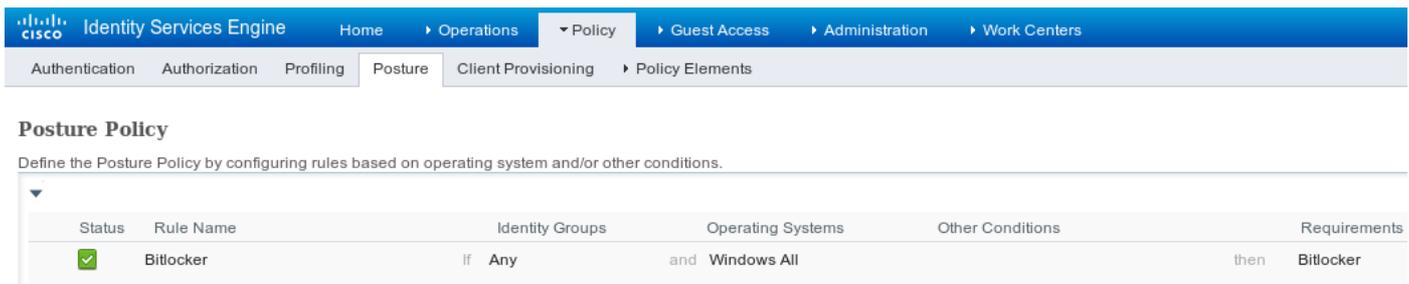
이 조건은 Windows 7용 BitLocker가 설치되어 있는지, E가 설치되어 있는지 확인합니다. 파티션이 완전히 암호화되었습니다.

**참고:**BitLocker는 디스크 수준 암호화이며 경로 인수가 있는 특정 위치를 지원하지 않으며 디스크 문자만 지원합니다.

이미지에 표시된 상태를 사용하는 새 요구 사항을 생성하려면 Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Posture(포스처) > Requirements(요구 사항)로 이동합니다.

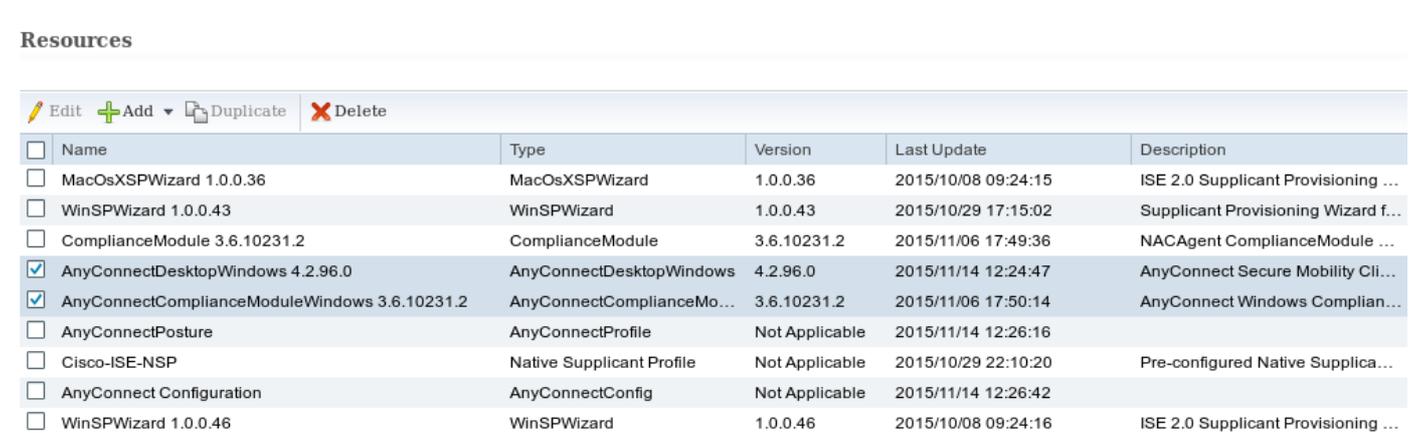


Policy(정책) > Posture(포스처)로 이동하여 이미지에 표시된 요구 사항을 사용하기 위해 모든 Windows에 대한 조건을 추가합니다.



### 3단계. 클라이언트 프로비저닝 리소스 및 정책

Policy(정책) > Policy Elements(정책 요소) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고, Cisco.com에서 Compliance Module(컴플라이언스 모듈)을 다운로드하고, 이미지에 표시된 대로 AnyConnect 4.2 패키지를 수동으로 업로드합니다.



Add(추가) > NAC Agent(NAC 에이전트) 또는 AnyConnect Posture Profile(AnyConnect 포스처 프로파일)로 이동하고 AnyConnect Posture 프로파일(이름:AnyConnectPosture) 기본 설정을 사용합니다.

Add(추가) > AnyConnect Configuration(AnyConnect 컨피그레이션)으로 이동하고 AnyConnect 프로필을 추가합니다(이름:이미지에 표시된 대로 AnyConnect 컨피그레이션)

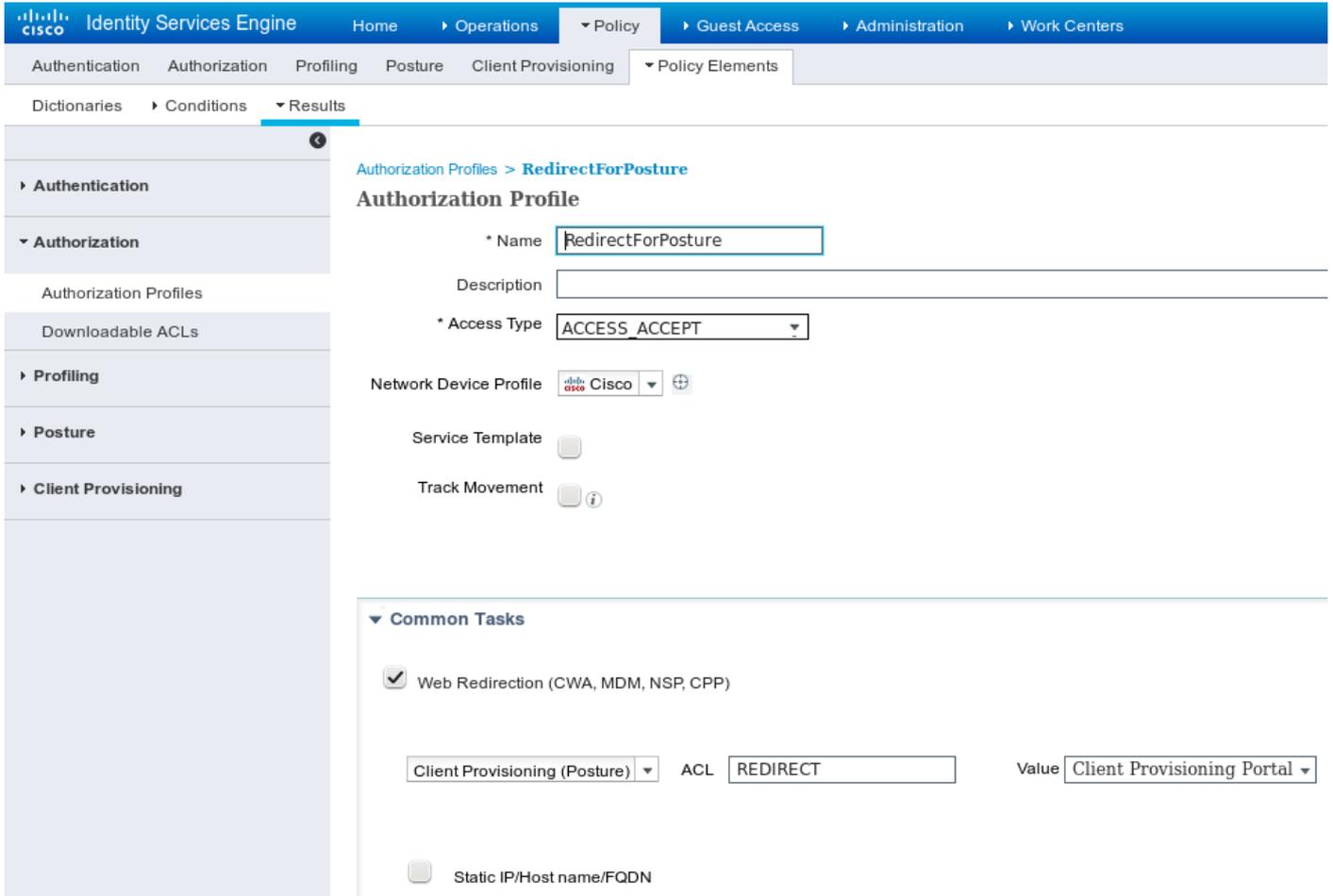
Policy(정책) > Client Provisioning(클라이언트 프로비저닝)으로 이동하고 이미지에 표시된 대로 구성된 AnyConnect 프로파일을 사용하려면 Windows에 대한 기본 정책을 수정합니다.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	if Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	if Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows	if Any	and Windows All	and Condition(s)	then AnyConnect Configuration
MAC OS	if Any	and Mac OSX	and Condition(s)	then MacOsXSPWizard 1.0.0.36 And Cisco-ISE-NSP

#### 4단계. 권한 부여 규칙

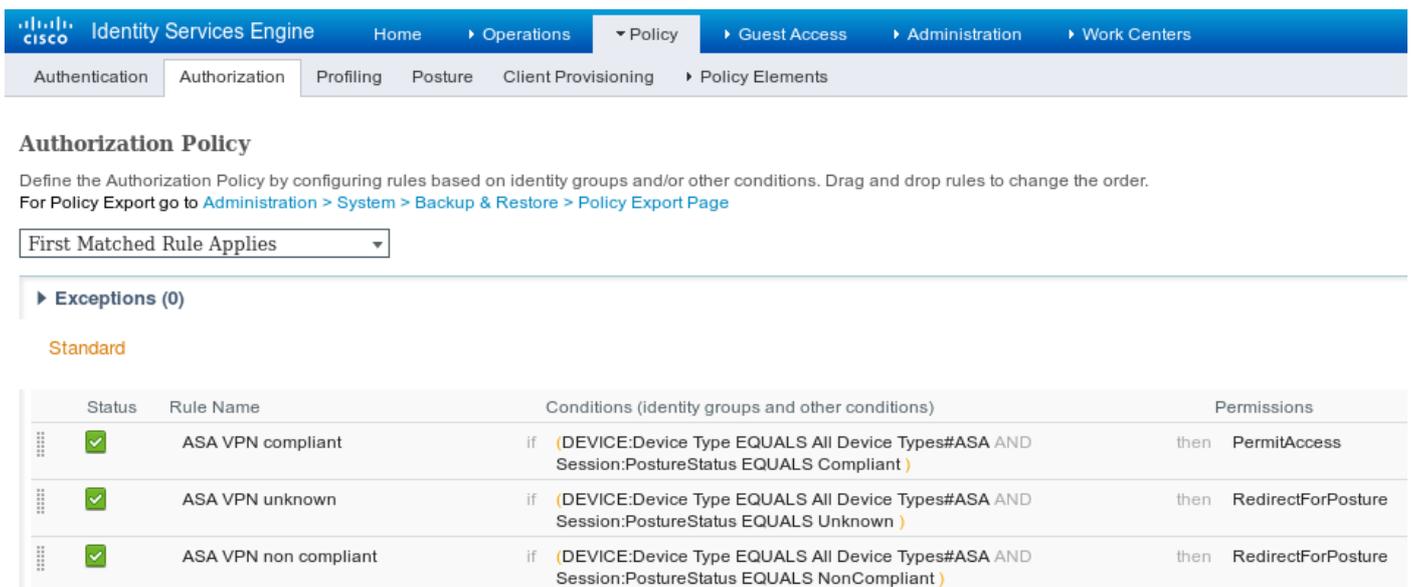
Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여)으로 이동하

고 Authorization Profile(권한 부여 프로파일)을 추가합니다(이름:RedirectForPosture) - 이미지에 표시된 대로 기본 클라이언트 프로비저닝 포털로 리디렉션됩니다.



리디렉션 ACL은 ASA에서 정의됩니다.

Policy(정책) > Authorization(권한 부여)으로 이동하여 이미지에 표시된 대로 3개의 권한 부여 규칙을 생성합니다.



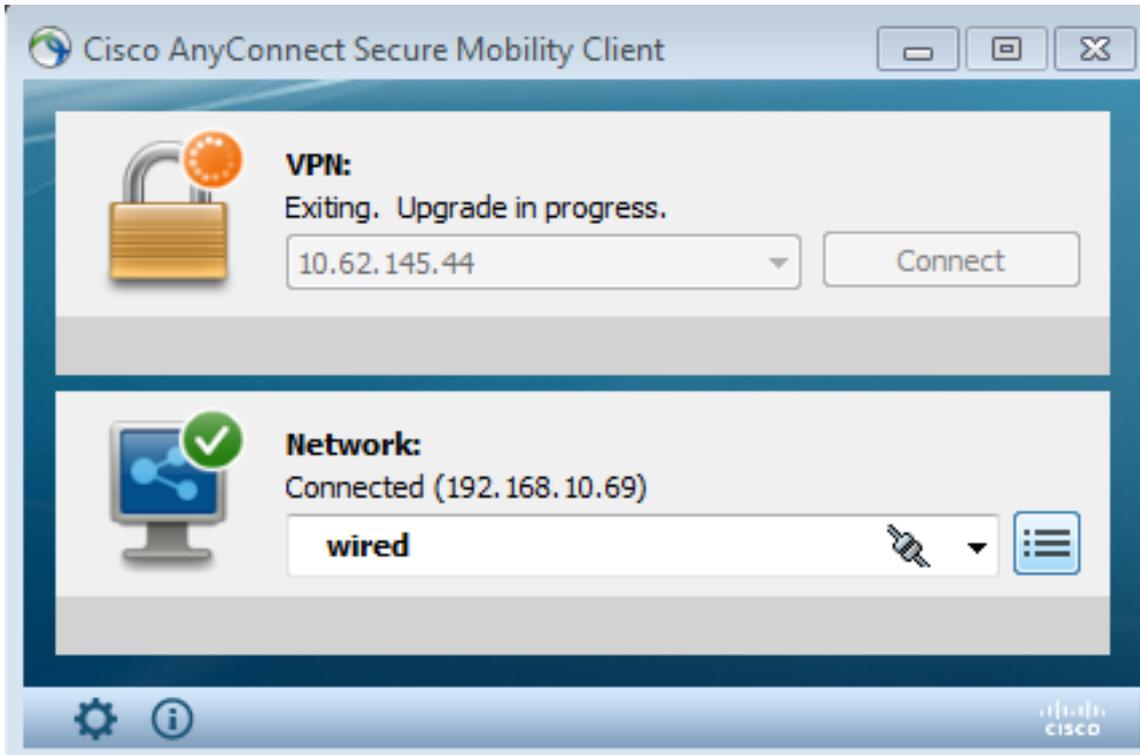
엔드포인트가 규정을 준수하는 경우 전체 액세스가 제공됩니다.상태를 알 수 없거나 규정을 준수하지 않으면 클라이언트 프로비저닝에 대한 리디렉션이 반환됩니다.

# 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

## 1단계. VPN 세션 설정

VPN 세션이 설정되면 ASA는 이미지에 표시된 대로 AnyConnect 모듈의 업그레이드를 수행할 수 있습니다.



ISE에서 마지막 규칙이 적용되면 이미지에 표시된 대로 RedirectForPosture 권한이 반환됩니다.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-11-14 14:59:06...	✓				10.229.20.45		PermitAccess	ASA	Dynamic Authorization succeeded
2015-11-14 14:59:04...	ⓘ		0	cisco	08:00:27:81:50:86	Default >> ASA VP...	RedirectForPosture		Session State is Postured
2015-11-14 14:58:22...	✓			cisco	08:00:27:81:50:86	Default >> ASA VP...	RedirectForPosture	ASA	Authentication succeeded

ASA가 VPN 세션 구축을 완료하면 리디렉션이 발생해야 한다고 보고합니다.

```
ASAv# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : cisco                Index          : 32
Assigned IP   : 172.16.31.10         Public IP      : 10.61.90.226
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
```

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 53201 Bytes Rx : 122712  
Pkts Tx : 134 Pkts Rx : 557  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : AllProtocols Tunnel Group : TAC  
Login Time : 21:29:50 UTC Sat Nov 14 2015  
Duration : 0h:56m:53s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : c0a80101000200005647a7ce  
Security Grp : none

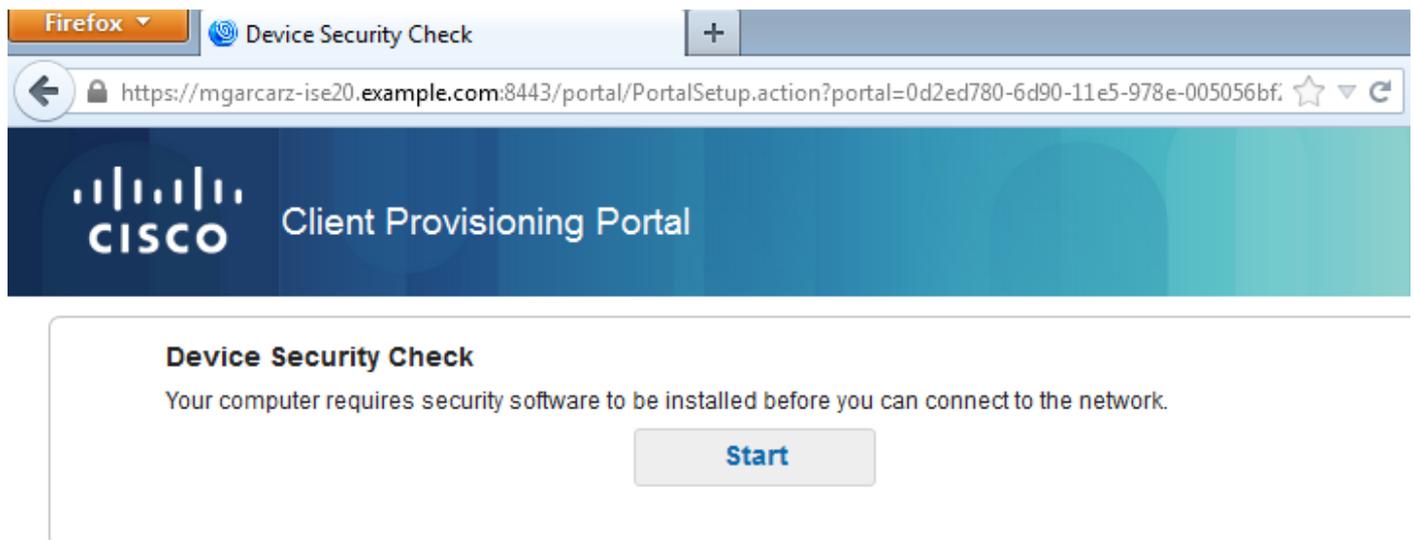
<some output omitted for clarity>

#### ISE Posture:

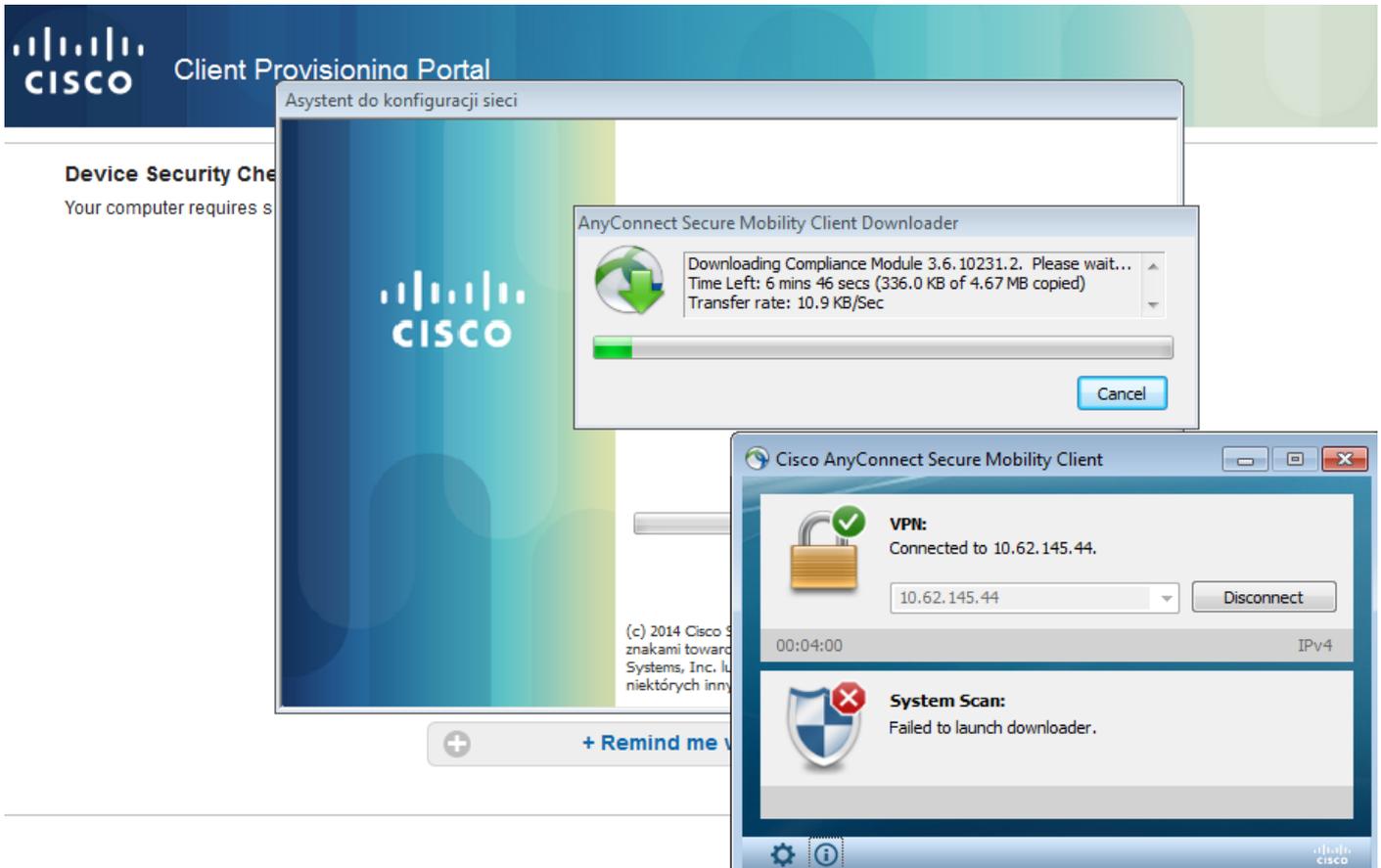
Redirect URL : <https://mgarcarz-ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-005056bf>  
Redirect ACL : REDIRECT

## 2단계. 클라이언트 프로비저닝

이 단계에서 엔드포인트 웹 브라우저 트래픽은 이미지에 표시된 대로 클라이언트 프로비저닝을 위해 ISE로 리디렉션됩니다.

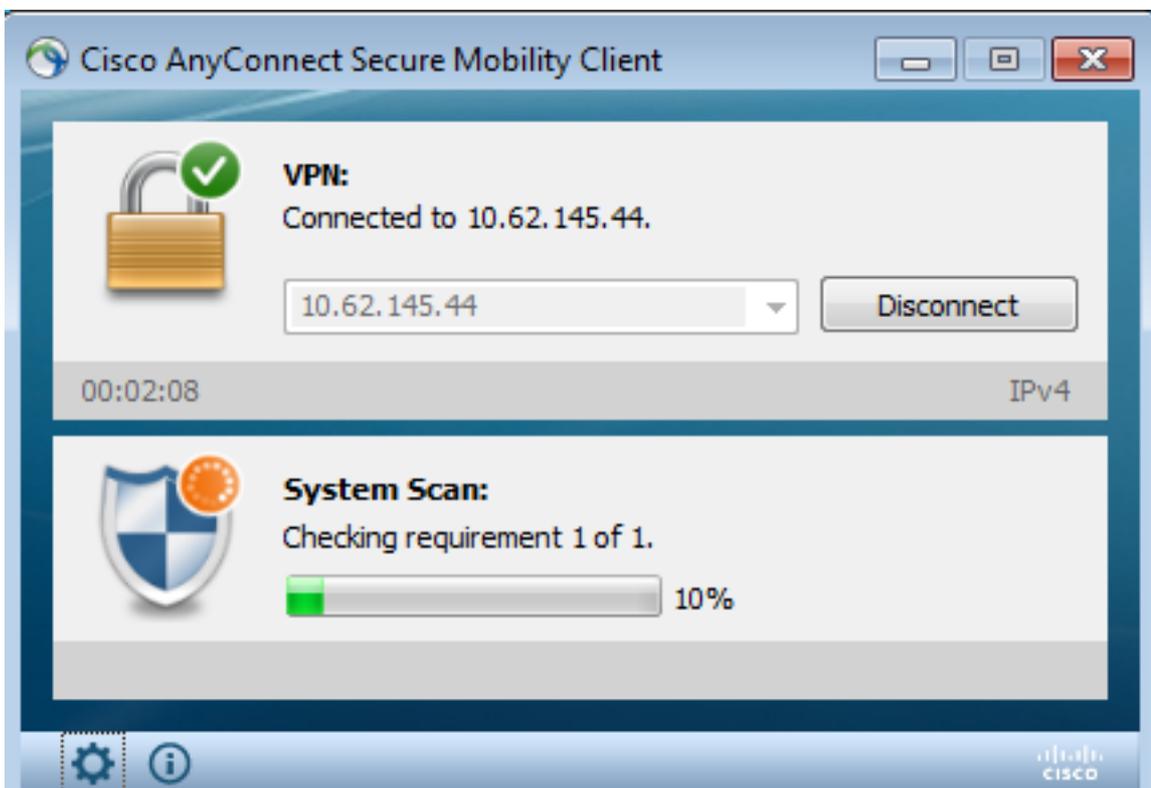


필요한 경우 AnyConnect가 Posture 및 Compliance 모듈과 함께 이미지에 표시된 대로 업데이트됩니다.

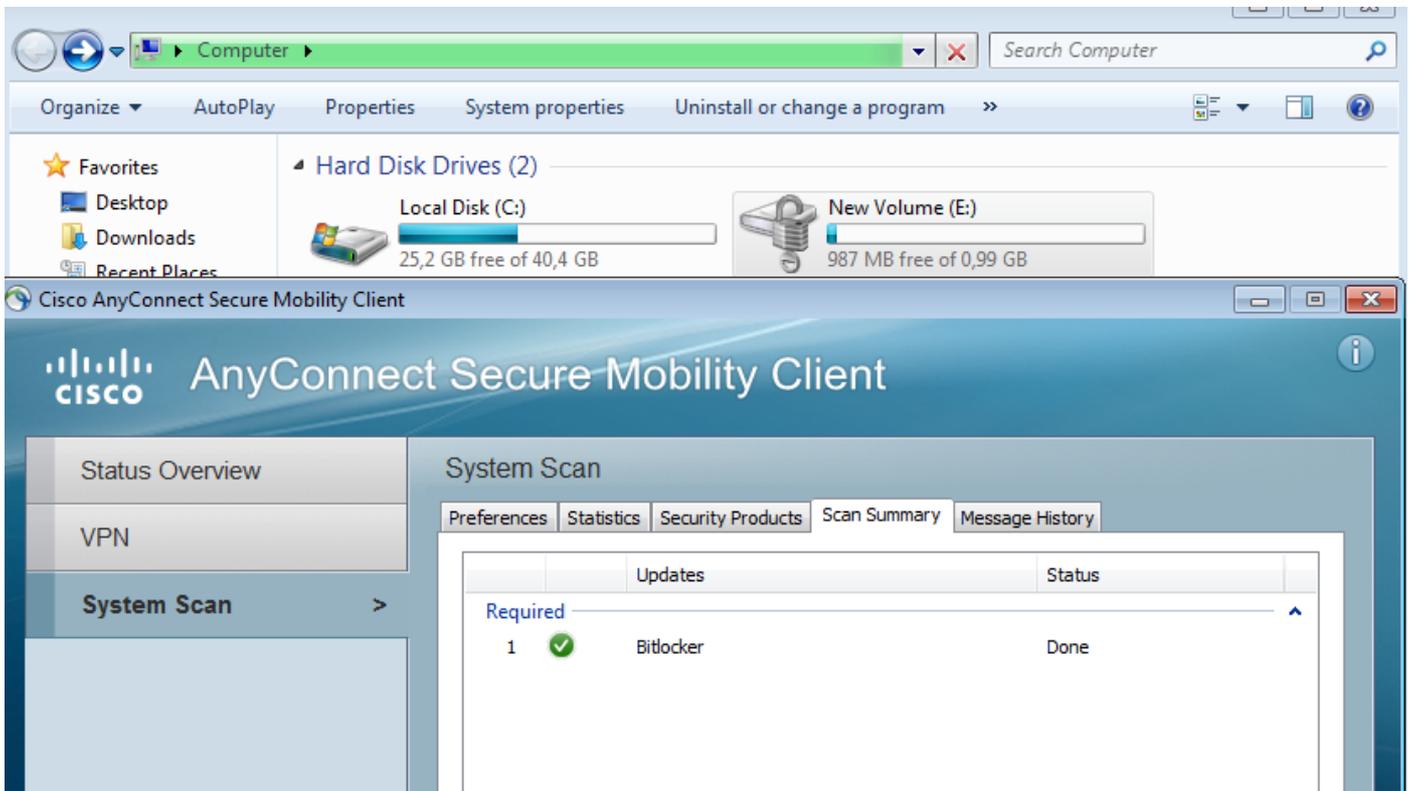


### 3단계. 상태 확인 및 CoA

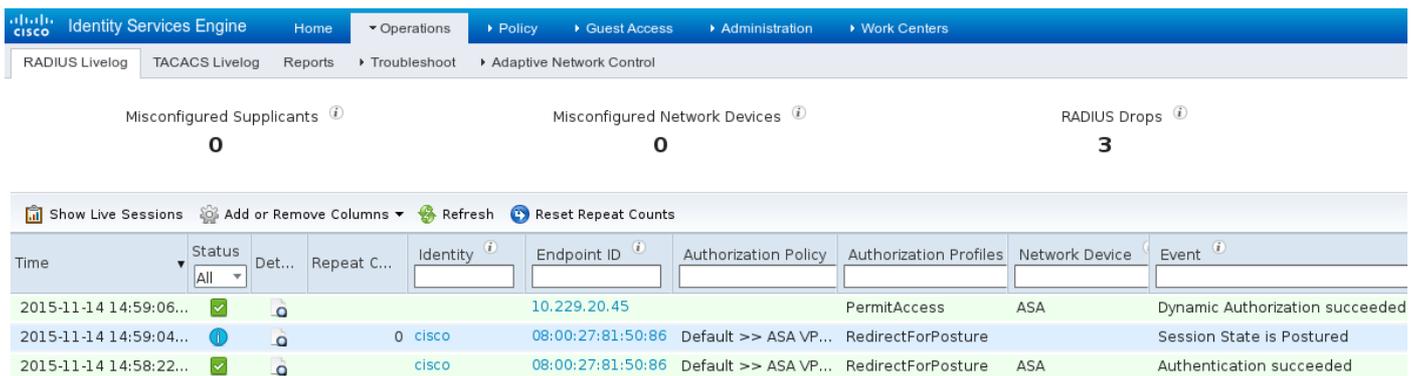
포스처 모듈이 실행되고 ISE를 검색합니다(성공하려면 enroll.cisco.com에 대한 DNS A 레코드가 필요할 수 있음). 이미지에 표시된 상태 조건을 다운로드 및 확인합니다.



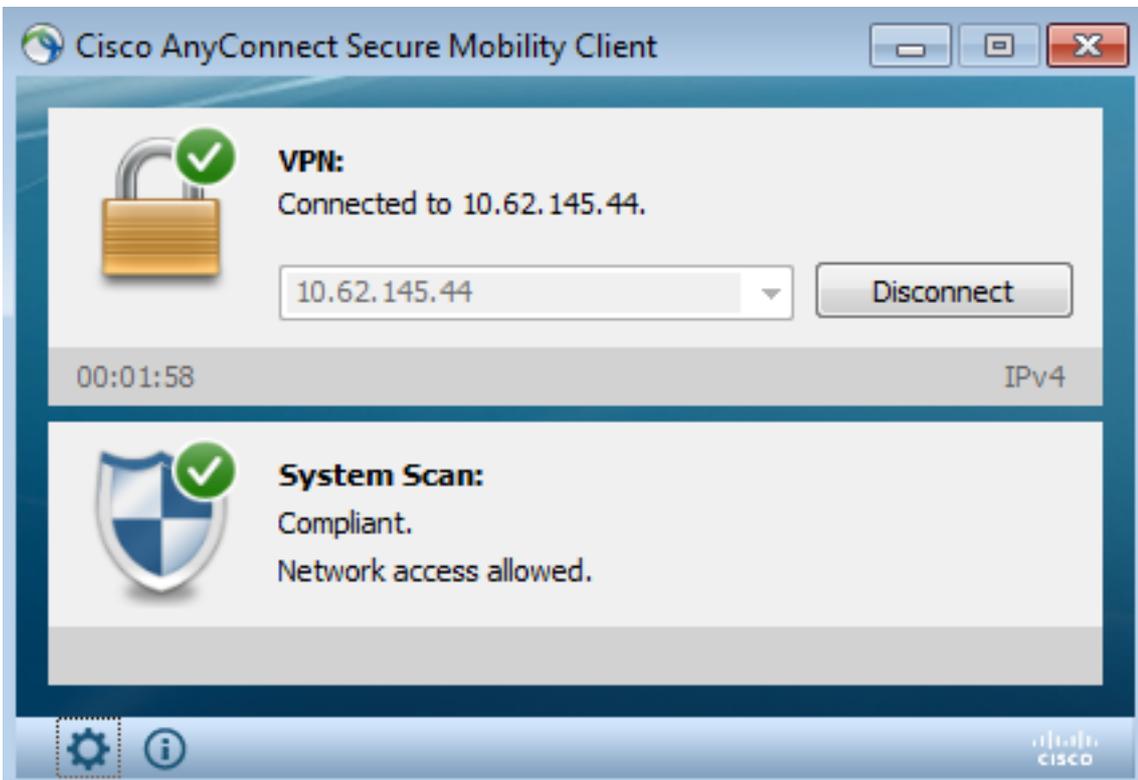
일단 E가 확인되면 파티션은 BitLocker에 의해 완전히 암호화되며, 이미지에 표시된 대로 올바른 보고서가 ISE로 전송됩니다.



이렇게 하면 이미지에 표시된 대로 CoA가 VPN 세션을 재인증하도록 트리거됩니다.



ASA는 전체 액세스를 제공하는 리디렉션 ACL을 제거합니다. AnyConnect는 이미지에 표시된 대로 규정준수를 보고합니다.



또한 ISE에 대한 상세 보고서는 두 조건이 모두 충족되었음을 확인할 수 있습니다(**Posture Assessment by Condition**은 모든 조건을 표시하는 새 ISE 2.0 보고서입니다). 첫 번째 조건 (**hd\_inst\_BitLockerDriveEncryption\_6\_x**)은 설치/프로세스를 확인하며 두 번째 조건 (**hd\_loc\_bitlocker\_specific\_1**)은 이미지에 표시된 대로 특정 위치(E:)가 완전히 암호화되었는지 확인합니다.

Report Selector	Posture Assessment by Condition									
<ul style="list-style-type: none"> <li>Identity Services Engine</li> <li>Home</li> <li>Operations</li> <li>Policy</li> <li>Guest Access</li> <li>Administration</li> <li>Work Centers</li> <li>RADIUS Livelog</li> <li>TACACS Livelog</li> <li>Reports</li> <li>Troubleshoot</li> <li>Adaptive Network Control</li> </ul>	Logged At	Postur	Identity	Endpoint ID	IP Address	Endpoint OS	Policy	Enforcement	Condition Status	Condition name
<ul style="list-style-type: none"> <li>ISE Reports</li> <li>Audit (10 reports)</li> <li>Device Administration (4 reports)</li> <li>Diagnostics (10 reports)</li> <li>Endpoints and Users</li> <li>Authentication Summary</li> <li>Client Provisioning</li> <li>Current Active Sessions</li> <li>External Mobile Device Management</li> <li>Identity Mapping</li> <li>Manual Certificate Provisioning</li> <li>Posture Assessment by Condition (Filters)</li> <li>Time Range: Today</li> <li>Run</li> <li>Posture Assessment by Endpoint</li> </ul>	2015-11-14 14:59:04.8	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_loc_bitlocker_specific_1
	2015-11-14 14:59:04.8	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:42:25.7	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:42:25.7	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_1
	2015-11-14 14:38:46.1	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:38:46.1	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_1
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_2
	2015-11-14 14:35:32.3	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:35:32.3	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1
	2015-11-14 14:32:07.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:32:07.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1

엔드포인트별 ISE 상태 평가 보고서는 이미지에 표시된 대로 모든 조건이 충족되었음을 확인합니다.

## Posture More Detail Assessment

Time Range: From 11/14/2015 12:00:00 AM to 11/14/2015 11:42:08 PM  
Generated At: 2015-11-14 23:42:08.257

### Client Details

Username:	cisco
Mac Address:	08:00:27:81:50:86
IP address:	10.62.145.44
Session ID:	c0a801010001700056473ebe
Client Operating System:	Windows 7 Ultimate 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.2.00096
PRA Enforcement:	0
CoA:	Received a posture report from an endpoint
PRA Grace Time:	0
PRA Interval:	0
PRA Action:	N/A
User Agreement Status:	NotEnabled
System Name:	ADMIN-KOMPUTER
System Domain:	n/a
System User:	admin
User Domain:	admin-Komputer
AV Installed:	
AS Installed:	Windows Defender;6.1.7600.16385;1.141.3676.0;01/11/2013;

### Posture Report

Posture Status:	Compliant
Logged At:	2015-11-14 14:59:04.827

ise-psc.log 디버그에서도 이를 확인할 수 있습니다.ISE에서 받은 상태 요청 및 응답:

```
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::c0a801010001700056473ebe::- Received posture request [parameters: reqtype=validate, userip=10.62.145.44, clientmac=08-00-27-81-50-86, os=WINDOWS, osVerison=1.2.1.6.1.1, architecture=9, provider=Device Filter, state=, ops=1, avpid=, avvname=Microsoft Corp.:!::!::!::!, avpname=Windows Defender:!::!::!::!, avpversion=6.1.7600.16385:!::!::!::!, avpfeature=AS:!::!::!::!, userAgent=Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.1; AnyConnect Posture Agent v.4.2.00096), session_id=c0a801010001700056473ebe
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Creating a new session info for mac 08-00-27-81-50-86
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Turning on encryption for endpoint with mac 08-00-27-81-50-86 and os WINDOWS, osVersion=1.2.1.6.1.1
2015-11-14 14:59:01,974 DEBUG [portal-http-service28][]
```

```
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco:c0a801010001700056473ebe::- Agent criteria
for rule [Name=bitlocker, Description=, Operating Systems=[Windows All],
Vendor=com.cisco.cpm.posture.edf.AVASVendor@96b084e, Check Type=Installation, Allow older def
date=0, Days Allowed=Undefined, Product Name=[com.cisco.cpm.posture.edf.AVASProduct@44870fea]] -
( ( (hd_inst_BitLockerDriveEncryption_6_x) ) & (hd_loc_bitlocker_specific_1) )
```

상태 요구 사항(조건 + 교정)이 있는 응답은 XML 형식입니다.

```
2015-11-14 14:59:02,052 DEBUG [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
<version>2</version>
<encryption>0</encryption>
<package>
  <id>10</id>
```

```
</version/>
```

```
<type>3</type>
<optional>0</optional>
<action>3</action>
<check>
  <id>hd_loc_bitlocker_specific_1</id>
  <category>10</category>
  <type>1002</type>
  <param>180</param>
```

```
<value_type>2</value_type>
</check>
<check>
```

```
<category>10</category>
<type>1001</type>
<param>180</param>
<operation>regex match</operation>
```

```
<value>^6\..+$|^6$</value>
<value_type>3</value_type>
</check>
<criteria>( ( ( hd_inst_BitLockerDriveEncryption_6_x ) &
(hd_loc_bitlocker_specific_1 ) ) )</criteria>
</package>
</cleanmachines>
```

ISE에서 암호화된 보고서를 받은 후:

```
2015-11-14 14:59:04,816 DEBUG [portal-http-service28][
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypting
report
2015-11-14 14:59:04,817 DEBUG [portal-http-service28][
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypted
report [
<report><version>1000</version><encryption>0</encryption><key></key><os_type>WINDOWS</os_type><
sversion>1.2.1.6.1.1</osversion><build_number>7600</build_number><architecture>9</architecture><
user_name>[device-filter-AC]</user_name><agent>x.y.z.d-todo</agent><sys_name>ADMIN-
KOMPUTER</sys_name><sys_user>admin</sys_user><sys_domain>n/a</sys_domain><sys_user_domain>admin-
Komputer</sys_user_domain><av><av_vendor_name>Microsoft
Corp.</av_vendor_name><av_prod_name>Windows
Defender</av_prod_name><av_prod_version>6.1.7600.16385</av_prod_version><av_def_version>1.141.36
76.0</av_def_version><av_def_date>01/11/2013</av_def_date><av_prod_features>AS</av_prod_features
></av><package><id>10</id><status>1</status><check><chk_id>hd_loc_bitlocker_specific_1</chk_id>
```

```
</check><check><chk_id>hd_inst_BitLockerDriveEncryption_6_x</chk_id><chk_status>1</check></pack
age></report> ]]
```

스테이션은 규정 준수로 표시되고 ISE는 CoA를 전송합니다.

```
2015-11-14 14:59:04,823 INFO [portal-http-service28][
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a801010001700056473ebe::- Posture state is
compliant for endpoint with mac 08-00-27-81-50-86
```

```
2015-11-14 14:59:06,825 DEBUG [pool-5399-thread-1][ cisco.cpm.posture.runtime.PostureCoA -
:cisco:c0a801010000f0005647358b::- Posture CoA is triggered for endpoint [08-00-27-81-50-86]
with session [c0a801010001700056473ebe
```

또한 ISE에서 최종 컨피그레이션을 전송합니다.

```
2015-11-14 14:59:04,827 DEBUG [portal-http-service28][
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Sending
response to endpoint 08-00-27-81-50-86 http response [ [ <!--X-Perfigo-DM-Error=0--><!--error=0--
><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--><!--X-Perfigo-Auto-Close-Login-
Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--><!--user role=--><!--X-Perfigo-OrigRole=--
><!--X-Perfigo-UserKey=dummykey--><!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-
Perfigo-Session=--><!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter--><!--X-
Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4--><!--X-Perfigo-DHCP-Renew-Delay=1--
><!--X-Perfigo-Client-MAC=08:00:27:81:50:86--> ]]
```

이러한 단계는 클라이언트 측(AnyConnect DART)에서도 확인할 수 있습니다.

```
Date : 11/14/2015
Time : 14:58:41
Type : Warning
Source : acvpnui
```

Description : Function: Module::UpdateControls

File: .\Module.cpp

Line: 344

No matching element found for updating: [System Scan], [label], [nac\_panel\_message\_history], [Scanning system ... ]

\*\*\*\*\*

Date : 11/14/2015  
Time : 14:58:43  
Type : Warning  
Source : acvpnuui

Description : Function: Module::UpdateControls  
File: .\Module.cpp  
Line: 344

No matching element found for updating: [System Scan], [label], [nac\_panel\_message\_history],  
[Checking requirement 1 of 1. ]

\*\*\*\*\*

Date : 11/14/2015  
Time : 14:58:46  
Type : Warning  
Source : acvpnuui

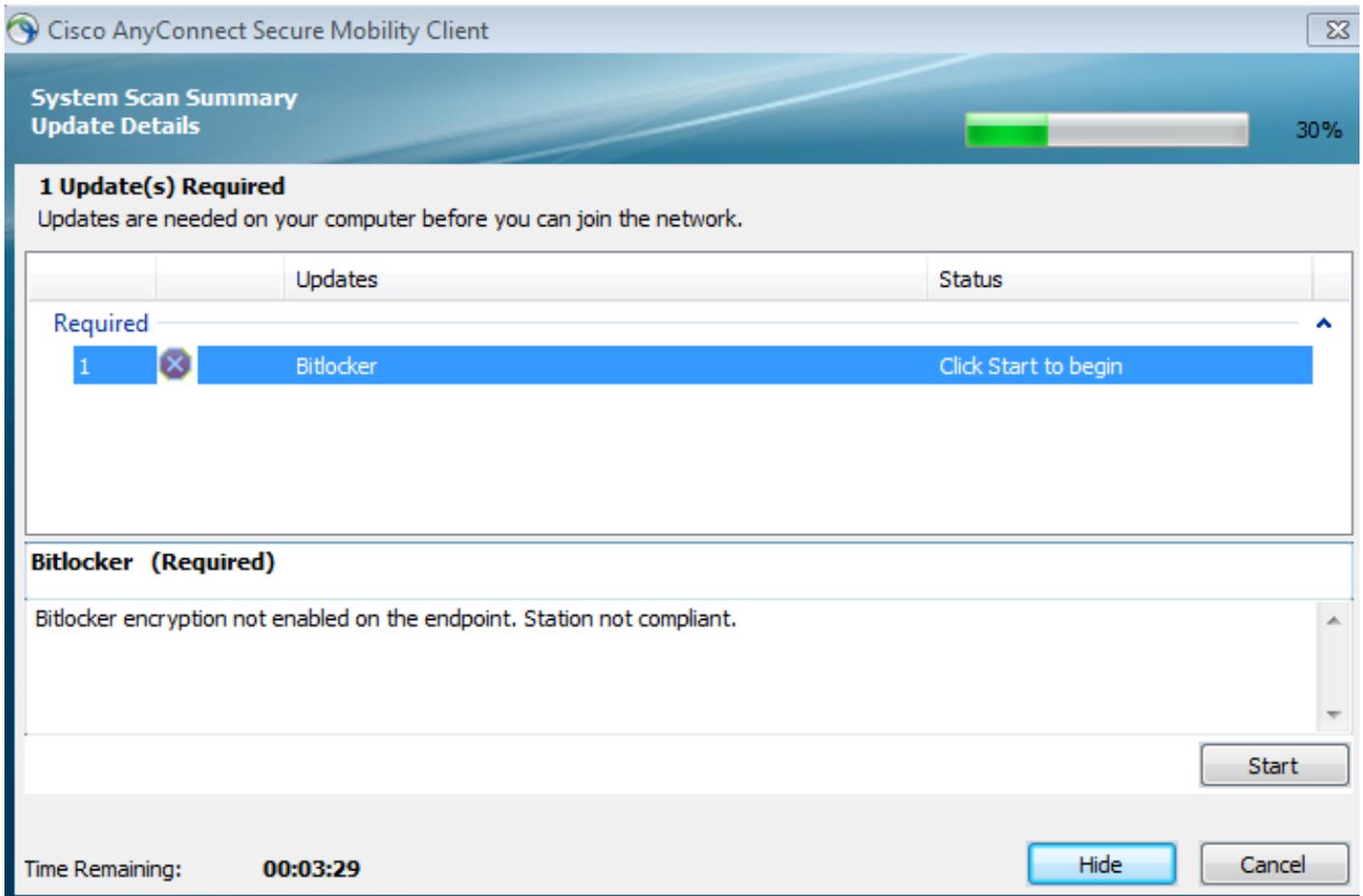
Description : Function: CMacApiShim::PostureNotification  
File: .\MacShim.cpp  
Line: 461

Clearing Posture List.

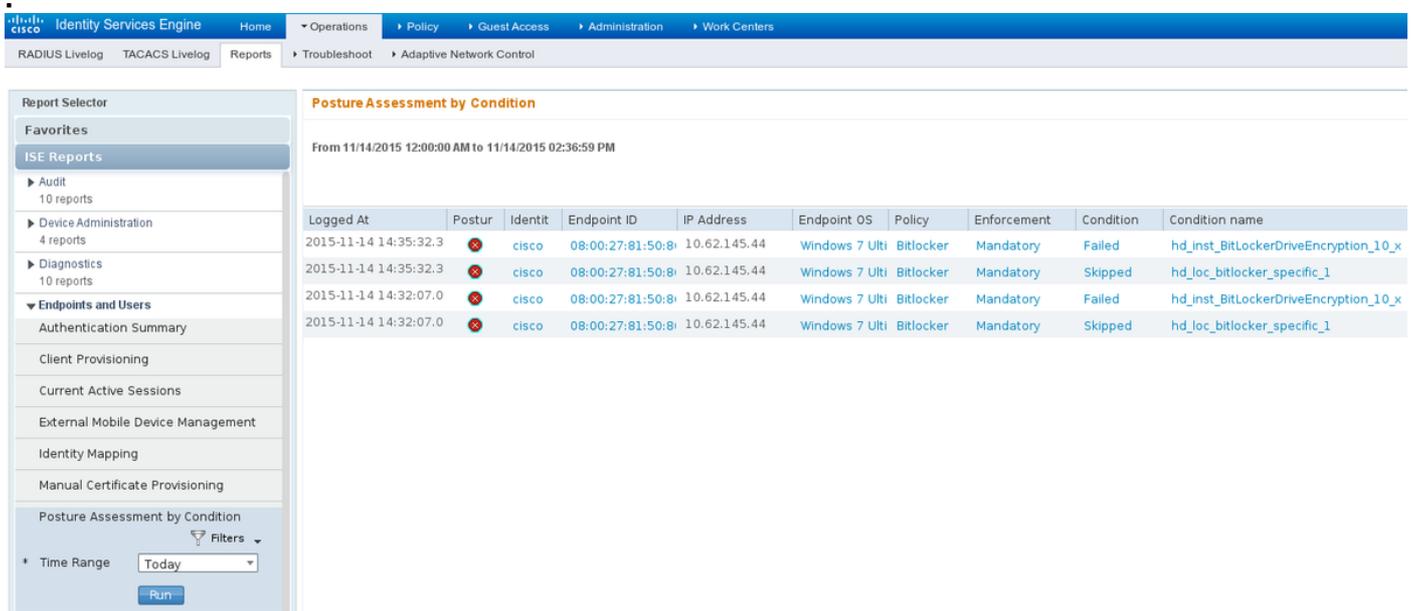
성공적인 세션을 위해 AnyConnect UI System Scan/Message History 보고서:

14:41:59 Searching for policy server.  
14:42:03 Checking for product updates...  
14:42:03 The AnyConnect Downloader is performing update checks...  
14:42:04 Checking for profile updates...  
14:42:04 Checking for product updates...  
14:42:04 Checking for customization updates...  
14:42:04 Performing any required updates...  
14:42:04 The AnyConnect Downloader updates have been completed.  
14:42:03 Update complete.  
14:42:03 Scanning system ...  
14:42:05 Checking requirement 1 of 1.  
14:42:05 Updating network settings.  
14:42:10 Compliant.

**버그** [CSCux15941](#) - ISE 2.0 및 AC4.2 Posture Bitlocker 암호화(위치 실패 시)(char \ / 지원되지  
않음) **문제 해결** 이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합  
니다. 엔드포인트가 규정을 준수하지 않는 경우 이미지에 표시된 대로 AnyConnect UI에서 보고(구  
성된 교정이 실행됨)합니다



ISE는 이미지에 표시된 대로 장애 상태에 대한 세부 정보를 제공할 수 있습니다



CLI 로그에서도 동일한 항목을 확인할 수 있습니다(예: Verify 섹션의 로그). **관련 정보**

- [보안 어플라이언스 사용자 권한 부여를 위한 외부 서버 구성](#)
- [Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.1](#)
- [Cisco Identity Services Engine 관리자 가이드, 릴리스 2.0](#)
- [기술 지원 및 문서 - Cisco Systems](#)